

1/3

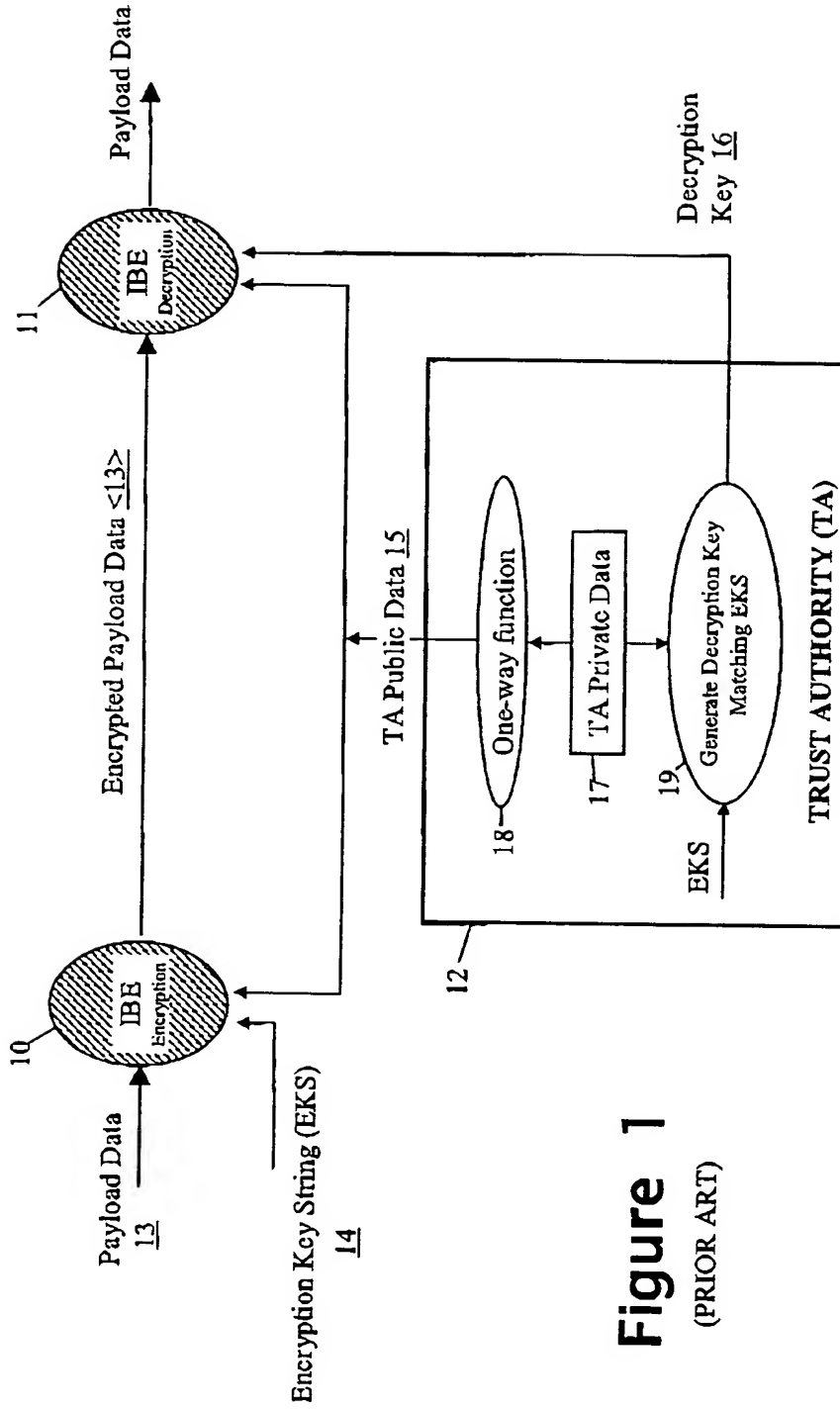
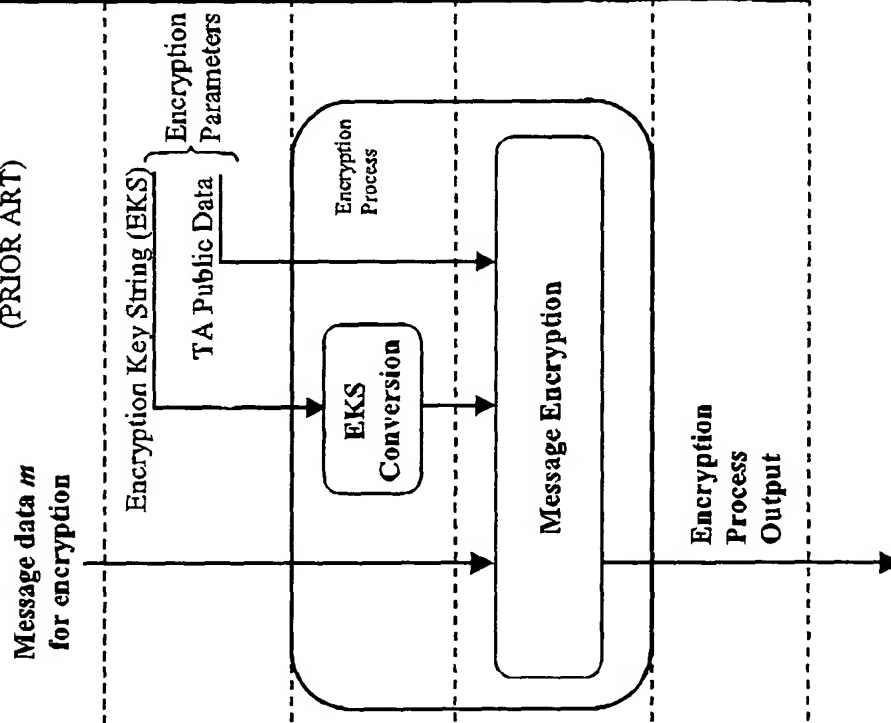


Figure 1
(PRIOR ART)

Figure 2
(PRIOR ART)



2/3

Identifier-Based Method			
Quadratic Residuosity	Bilinear Mappings	RSA Based	
	$\varphi: G_1 \times G_1 \rightarrow G_2$		
EKS	EKS	EKS	
Modulus N	(P, sP) where P is in G_1 s is secret of TA	Modulus n	
$K = \#(\text{EKS})$	"Map-to-point" hash $Q_{ID} = H_I(\text{EKS})$ where $H_I: \{0,1\}^* \rightarrow G_1$	$c = \#(\text{EKS}) \bmod n$	
For each bit: $s_+ \equiv (t_+ + K/t_+) \bmod N$ $s_- \equiv (t_- - K/t_-) \bmod N$	$V = m \oplus H_2(\varphi(sP, rQ_{ID}))$ where: $H_2: G_2 \rightarrow \{0,1\}^*$ r is a random number	$m^e \bmod n$	
For each bit: s_+, s_- (knowledge of EKS and TA concerned also needs to be available)	$V, U (= rP)$	$m^e \bmod n$	

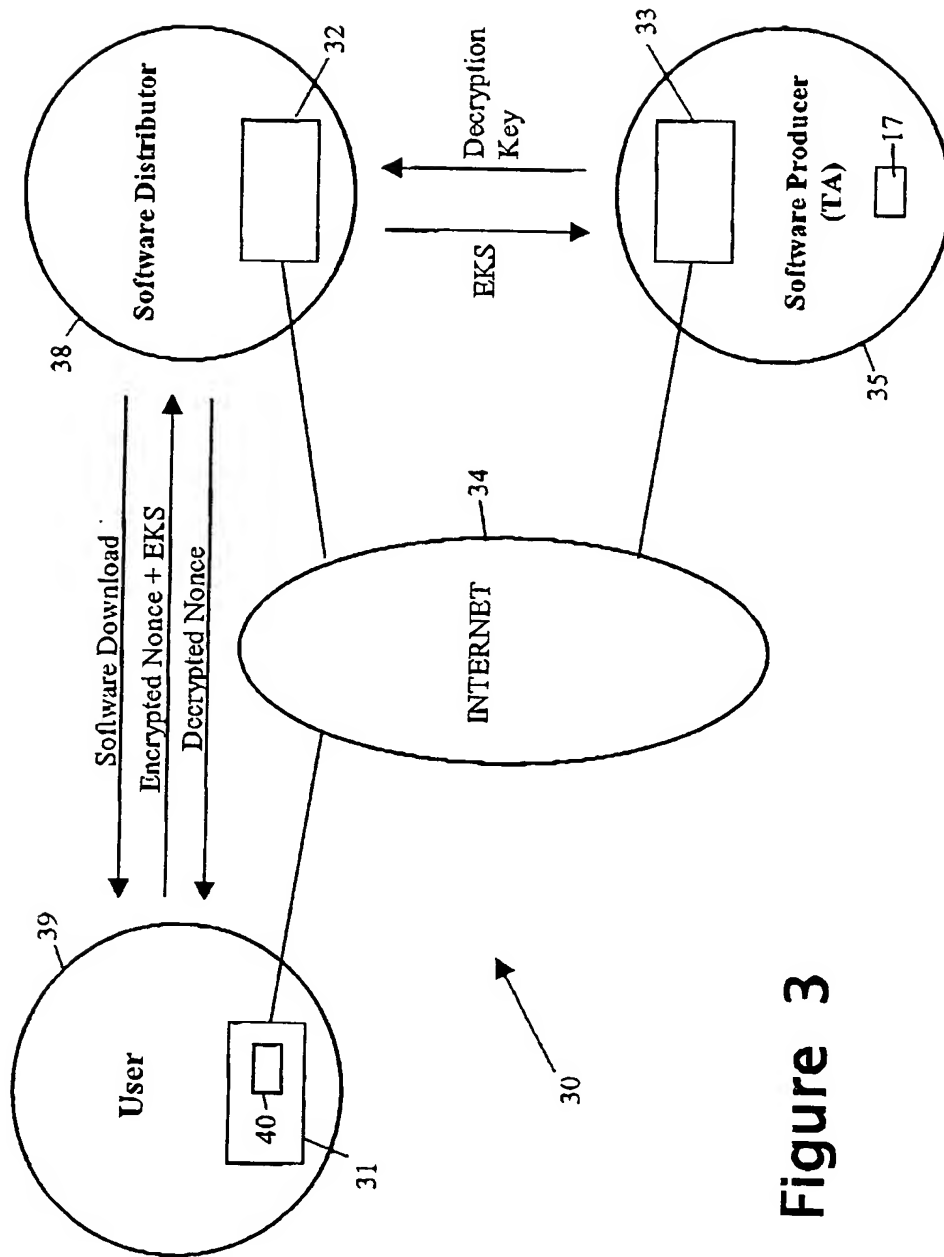


Figure 3